TPM for Dell Business Clients Using Self Contained Executable

A Dell Technical White Paper

Authors

Vibha Garg is an engineer in the Dell Open Manage Biz Client Organization.

Sharmad Naik is an engineer in the Dell Open Manage Biz Client Organization.

Sahid Md Shaik is an engineer in the Dell Open Manage Biz Client Organization.

Contents

Introduction

A Trusted Platform Module (TPM) is a type of hardware data protection provided by a microchip built into the computer. Microsoft Windows BitLocker Drive Encryption, a software data protection feature, is designed to work with a TPM.

Dell uses TPM to provide the Core Root of Trust for Measurement (CRTM) and Reporting for applications desiring the ability to verify that the system state has not changed and as the Root of Trust for Storage (RTS) for applications desiring a secure storage mechanism for rooting their encryption key hierarchies.

Dell Business Client Systems, for example: Latitude, Precision and Optiplex line PCs are shipped with the TPM chip.

CCTK and SCE

CCTK is a Dell tool used to configure BIOS settings on Dell Business Client systems.

SCE is a self-contained executable with .exe extension. SCE is just execute-only and does not install itself. It is a zero-touch program. SCE is created by CCTK user interface. SCE contains the configuration in a file that you export using CCTK user interface.

Scope

This white paper illustrates how to prepare an SCE to enable and activate TPM using the CCTK user interface.

This document is not intended to explain TPM. You should have knowledge of TPM.

Prerequisites

Below is the required system components list used to create a SCE:

- CCTK installed on a system
- .NET 3.5 sp1
- Administrator access
- Setup/Admin password is not set

Target machines:

- TPM must be present.
- Trusted Platform Module (TPM) must not be currently owned.
- TPM must be in deactivated state.
- Setup/Admin password is not set.

Note: Dell strongly recommends that customers continue to maintain an administrator password on systems that have TPM active.

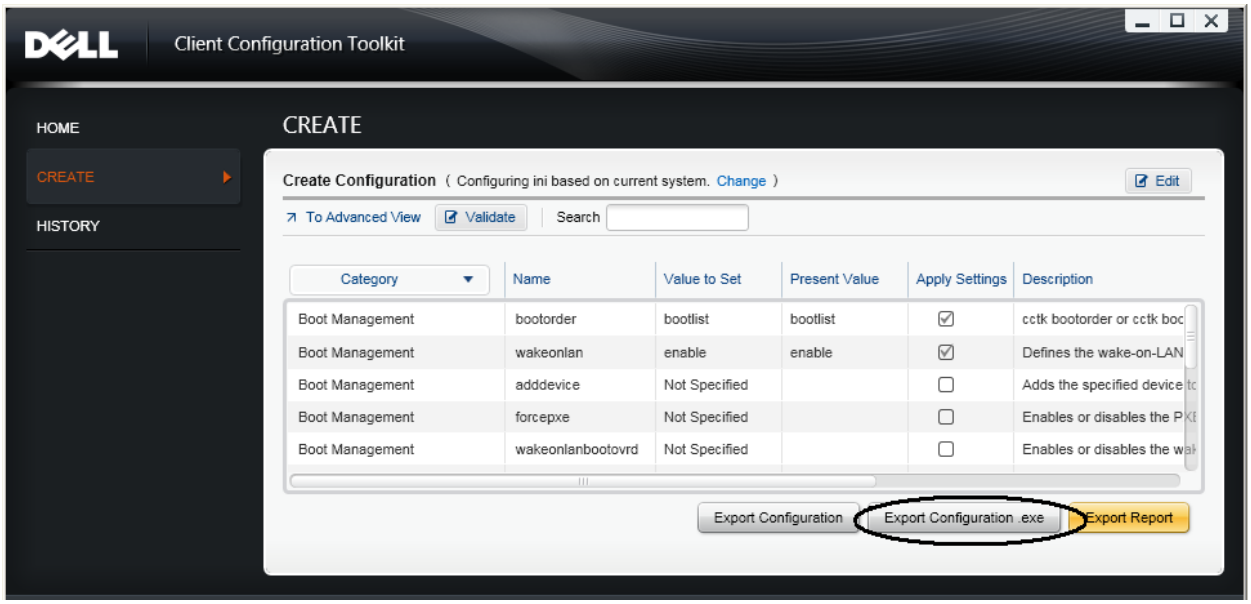
Download CCTK

Download CCTK as self-extractable file for Windows from http://support.dell.com. The most current release is CCTK 2.0. Check for the later release if available. In addition, CCTK is available directly as ftp.dell.com/sysman/Dell_CCTK_200_A00_R304287.exe.

Create an SCE with CCTK

Below are the detailed steps to create a SCE using the CCTK user interface.

1. Install CCTK to the default installation directory.
2. On the desktop, double-click on the **Dell Client Configuration Wizard** Icon, or Click on **Start->Programs->Dell->CTK->CCTK Configuration Wizard**.
3. Once the user interface comes up, click **Create Package**.
4. Next select one of the following options, the usage details of each are as follows:
   a. **Multi-Platform File**:
   Use this when you want to define your set of token to be applied from scratch i.e. you are not carrying any token from the host or earlier configurations
   b. **This System's File**:
   Use this when you did like to use the tokens defined on the current host system.
   c. **A Saved File**:
   Use this when you did like to use the tokens defined earlier in a CCTK configuration file saved earlier as .cctk/.ini file.
4. Choose the desired set of tokens and set their values in the configuration page and then click **Export Configuration .exe**.



5. Save the **SCE/EXE** in a folder on the hard drive.

Running SCE on the Target System

The SCE is a standalone program you run directly on the client machine using a command. For more information refer to section *Applying SCE on the target system* in the *CCTK User Guide* document.

Using SCE for TPM Settings

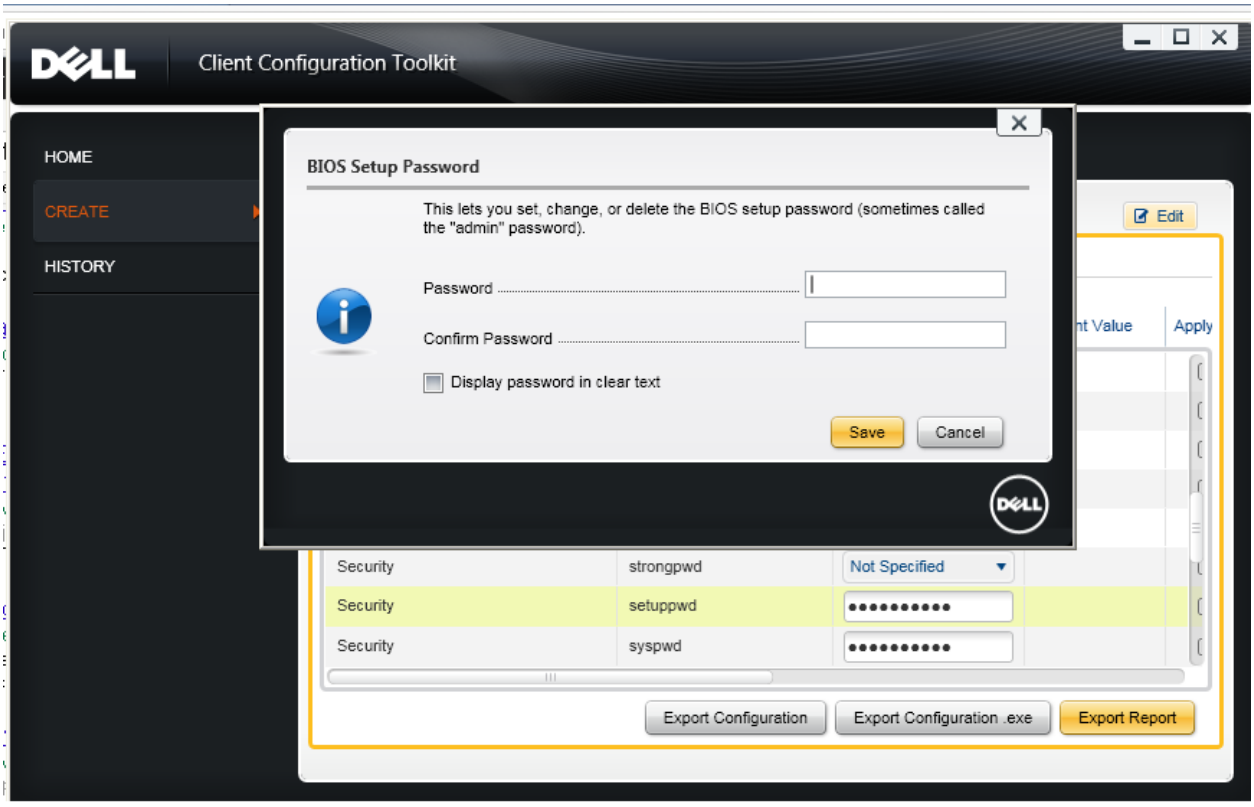
To activate the TPM setting using SCE, you need to generate two SCE files. The first SCE file sets the BIOS password on the target machine. The second SCE file activates and enables the TPM on the machine using the BIOS password provided at the time of SCE generation.

Generate the First SCE File to Set the BIOS Setup Password

Use these steps to generate the first SCE file, which sets the BIOS setup password.

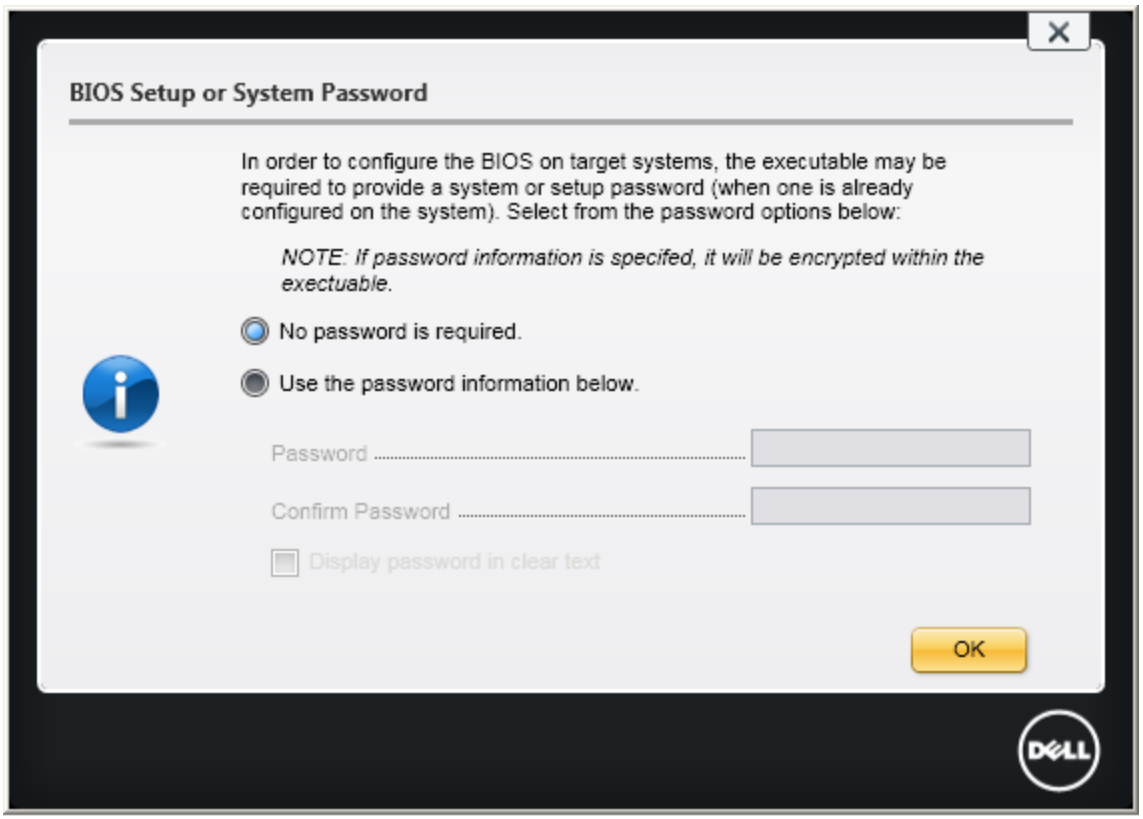
1. Create Package->This System's File->Next.
2. Search for the string *setuppwd*.
3. Double click on the highlighted row.
4. In the BIOS Setup Password dialog box, enter the values for password.
5. Click **Save.**

Figure 1. **Setting the BIOS Setup Password.**



6. Click **Export configuration .exe.**
7. Select **No password is required.**
8. Click **OK.**

Figure 2. **Selecting the No Password is Required Option.**



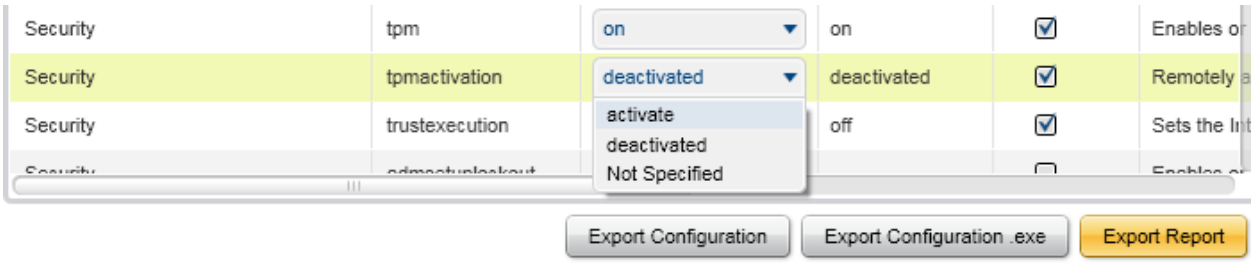
9. Save the SCE file.

Generate the Second SCE for TPM

Use these steps to generate the second SCE file.

1. Create Package->This System's File->Next.
2. Search for the string ***tpm***.
3. Set the ***tpm*** to ***on*** and ***tpmactivation*** to ***activate***.

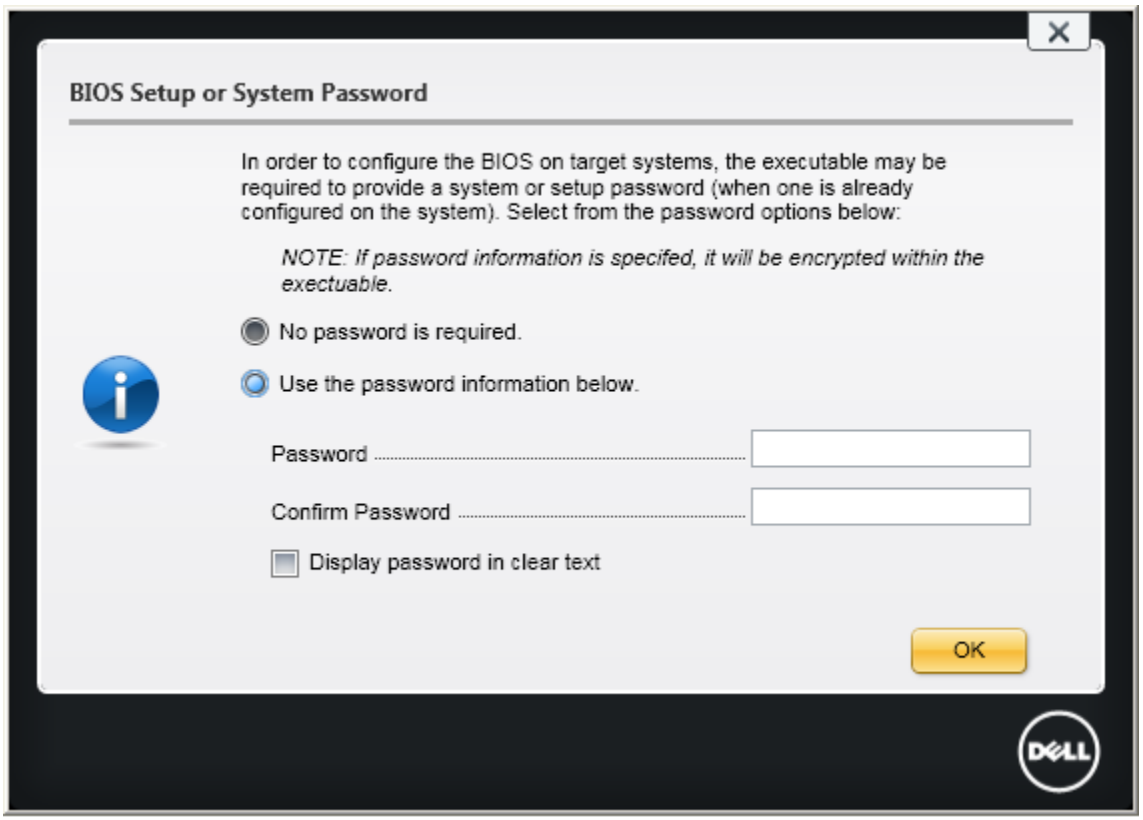
Figure 3. Setting the tpm to on and tpmactivation to activate.



4. Click **Export configuration .exe**.

5. Select **Use the Password information below** and enter the same password as in step 5 of first SCE.

Figure 4. Enter the same password as the previous procedure.



6. Save the SCE file.

Applying the SCEs on the Target System for TPM

Use these steps to apply the SCE files on the target system.

1. Execute the first SCE.
2. Execute the second SCE.
3. Reboot to operating system.

Note: Do not go to the system BIOS (F2).

Understanding the SCE LOG

When SCE is applied a log is generated. The log is found in the same directory as SCE with the name as *SCE*. It provides details of the tokens applied to target systems.

Additional Resources

The Dell Custom Factory Integration (CFI) process lets you enumerate and activate the TPM on all the new Dell systems you order by default. Contact your Dell account executive for more information.

Additional CCTK information is available from the following sources:

http://www.delltechcenter.com/page/Dell+Client+Configuration+Toolkit

Appendix

Sequence of steps to follow when setting TPM using the CCTK command line:

1. Set up the BIOS password: cctk --setuppwd=<password>.
2. TPM enable: cctk --tpm=on --valsetuppwd=<password>.
3. TPM Activate: cctk --tpmactivation=activate --valsetuppwd=<password>.
4. Reboot to OS.
5. TPM check: cctk --tpm --tpmactivation.